IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Arnold, et. al.	§ Group Art Unit: 2137
	§ Confirmation No.: 4841
	§ Examiner: Williams, Jeffery L
Serial No.: 10/099,779	§
	§ Attorney Docket No.
Filed: March 14, 2002	§ AUS920010984US1
	§
Title: System and Method for Using a Unique Identifier for Encryption Key Derivation	§ IBM Corporation § Intellectual Property Law § Dept. § 11400 Burnet Road § Austin, Texas 78758

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Mailing or Transmission

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 or electronically transmitted to the U.S. Patent and Trademark Office on the date shown below.

/Leslie A. Van Leeuwen, Reg. No. 42,196/ July 26, 2006
Leslie A. Van Leeuwen, Reg. No. 42,196 Date

APPELLANTS' BRIEF (37 CFR § 41.37)

Sir:

A. INTRODUCTORY COMMENTS

This brief is filed in support of the previously filed Notice of Appeal, filed in this case on June 5, 2006, which appealed from the decision of the Examiner dated March 3, 2006, finally rejecting claims 1, 6-8, 13, 14, and 19-29. Please charge the required fee under 37 CFR § 41.20(b)(2) to IBM Corporation Deposit Account No. 09-0447.

The two-month deadline for filing this Appeal Brief is August 5, 2006, therefore, no extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and the undersigned hereby authorizes the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

B. REAL PARTY IN INTEREST

The real party in interest in this appeal is International Business Machines Corporation, which is the assignee of the entire right, title, and interest in the above-identified patent application.

C. RELATED APPEALS AND INTERFERENCES

With respect to other prior or pending appeals, interferences, or judicial proceedings that are related to, will directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such prior or pending appeals, interferences, or judicial proceeding known to Appellants, Appellants' legal representative, or assignee.

D. STATUS OF CLAIMS

1. Total number of claims in application

There are 16 claims pending. Three claims are independent claims (1, 8, and 14), and the remaining claims are dependent claims.

2. Status of all claims in application

- Claims canceled: 2-5, 9-13, 15-18
- Claims withdrawn from consideration but not canceled: none
- Claims pending: 1, 6-8, 14, and 19-29
- Claims allowed: None
- Claims rejected: 1, 6-8, 14, and 19-29

3. Claims on appeal

Claims 1, 6-8, 14, and 19-29 are on appeal.

E. STATUS OF AMENDMENTS

All amendments have been entered in this case. Amendments were made and entered after the Final Office Action that included canceling claim 13 and correcting antecedent basis issues in Appellants' independent claims.

F. SUMMARY OF CLAIMED SUBJECT MATTER

Appellants provide a concise summary of the claimed subject matter as follows. Claims 1, 8, and 14 are independent claims. Note that claims 1, 6-7, and 21-23 are method claims, claims 8, and 24-26 are information handling system claims, and claims 14, 19-20, and 27-29 are computer program product claims. Independent claims 8 and 14 include logic elements and means plus function limitations that correspond to the method steps set forth in independent claim 1. An information handling system capable of implementing Appellants' invention, as claimed in independent claim 8, is shown in Figure 8, and described in Appellants' specification on pages 25-26. Support for independent computer program product claim 14 is described in Appellants' specification on page 26. In addition, support for each of the method steps, logic elements, and means plus function limitations of the independent claims are discussed below. The specific citations to Appellants' Figures and Specification are meant to be exemplary in nature, and do not limit the scope of the claims. In particular, the citations below do not limit the scope of equivalents as provided under 35 U.S.C. § 112, sixth paragraph.

As claimed in independent claims 1, 8, and 14, Appellants claim a method, information handling system, and computer program product for receiving, at a security module, a first password corresponding to a software application (See Figure 1A, pages 9-11, Figure 2, pages 13-15, and Figure 7, page 23-25); generating, at the security module, a first mask value based on the first password (See Figure 1A, pages 9-11, Figure 2, pages 13-15, Figure 3, pages 15-18, and Figure 7, page 23-25); combining, at the security module, the first mask value with a first encryption key, wherein the first encryption key is derived from a generated key and a known value, the combining resulting in a tied key (See Figure 1A, pages 9-11, Figure 2, pages 13-15, Figure 3, pages 15-18, and Figure 7, page 23-25); encrypting, at the security module, the tied key using a second encryption key that is associated with the security module, the encrypting resulting in an encrypted tied key (See Figure 1A, pages 9-11, Figure 2, pages 13-15, Figure 3,

pages 15-18, and Figure 7, page 23-25); returning the encrypted tied key to the software application (See Figure 1B, pages 11-13, Figure 4, pages 18-20, and Figure 7, page 23-25); determining, at the software application, that the encrypted tied key corresponds to the security module (See Figure 1B, pages 11-13, Figure 4, pages 18-20, and Figure 7, page 23-25); in response to the determining, sending the encrypted tied key and a second password from the software application to the security module over a computer network, the second password being the same as the first password (See Figure 1B, pages 11-13, Figure 4, pages 18-20, and Figure 7, page 23-25); receiving, at the security module, the encrypted tied key and the second password from the software application (See Figure 1B, pages 11-13, Figure 4, pages 18-20, and Figure 7, page 23-25); in response to receiving the encrypted tied key and the second password, combining, at the security module, the encrypted tied key and the second password, the combining resulting in a recovered tied key (See Figure 1B, pages 11-13, Figure 4, pages 18-20, Figure 5, pages 20-22, and Figure 7, page 23-25); generating a second mask value based on the second password (See Figure 1B, pages 11-13, Figure 4, pages 18-20, Figure 5, pages 20-22, and Figure 7, page 23-25); separating a recovered encryption key from the recovered tied key using the second mask value, the recovered encryption key including a recovered generated key and a recovered known value (See Figure 1B, pages 11-13, Figure 4, pages 18-20, Figure 5, pages 20-22, and Figure 7, page 23-25); and encrypting data provided by the software application using the recovered generated key (See Figure 1B, pages 11-13, Figure 4, pages 18-20, Figure 6, pages 22-23, and Figure 7, page 23-25).

G. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1, 6, 7, 8, 14, 19, 20, and 22 on appeal stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Al-Salqan (U.S. Patent No. 6,549,626, hereinafter "Al-Salqan") in view of Hosokawa (U.S. Patent Pub. 2001/0023416, hereinafter "Hosokawa"). Claims 21, 23-24, 26-27, and 29 on appeal stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Al-Salqan in view of Hosokawa and further in view of admission of Appellants' admitted prior art.

H. ARGUMENT

1. Claims 1, 6, 7, 8, 14, 19, 20, and 22 Are Patentable over Al-Salqan in view of Hosokawa. Claims 21, 23-24, 26-27, and 29 Are Patentable over Al-Salqan in view of Hosokawa and Further in view of Admission of Appellants' Admitted Prior Art

Independent claims 1, 8, and 14 claim a method, system, and program product for creating source code. Using claim 1 as an exemplary claim, each of these independent claims includes the limitations of:

1) receiving, at a security module, a first password corresponding to **a software application**;

2) generating, at the security module, a first mask value based on the first password;

3) combining, at the security module, the first mask value with a first encryption key, wherein the first encryption key is derived from a generated key and a known value, the combining resulting in a tied key;

4) encrypting, at the security module, the tied key using a second encryption key that is associated with the security module, the encrypting resulting in an encrypted tied key;

5) returning the encrypted tied key to **the software application**;

6) determining, **at the software application**, that the encrypted tied key corresponds to the security module;

7) in response to the determining, sending the encrypted tied key and a second password from **the software application** to the security module over a computer network, the second password being the same as the first password;

8) receiving, at the security module, the encrypted tied key and the second password from **the software application**;

9) in response to receiving the encrypted tied key and the second password, combining, at the security module, the encrypted tied key and the second password, the combining resulting in a recovered tied key;

10) generating a second mask value based on the second password;

11) separating a recovered encryption key from the recovered tied key using the second mask value, the recovered encryption key including a recovered generated key and a recovered known value; and

12) encrypting data provided by **the software application** using the recovered generated key.

Appellants use a security module to encrypt and decrypt data retrieved from a software application. Before the software application provides the data to the security module, the security module first creates an encrypted tied key and sends the encrypted tied key to the software application. The encrypted tied key is generated using a password corresponding to the software application along with an encryption key that is associated with the security module. Claim 1's first through fifth elements claim the software application providing a first password to the security module and, in turn, the security module providing the encrypted tied key, which has been encrypted with a second encryption key that is associated with the security module, to the software application.

Next, in claim 1's sixth element, the software application determines that the encrypted tied key corresponds to the security module. Appellants' invention then proceeds to send the encrypted tied key and the software application password back to the security module in order for the security module to extract a recovered generated key (seventh through eleventh

elements). Finally, Appellants' invention encrypts data, which is provided by the software application, using the recovered generated key (twelfth element).

Appellants assert that the Office Action fails to show that the prior art references teach or suggest all of Appellants' claim limitations. In particular, Appellants assert that the Office Action fails to view Appellants' invention as a "whole." MPEP 2141 states that "When applying 35 U.S.C. 103, the following tenets of patent law must be adhered to: (A) The claimed invention must be considered **as a whole**..." In addition, MPEP 2143.03 states:

> "To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art...**All words** in a claim must be considered in judging the patentability of that claim against the prior art" (emphasis added)

Appellants assert that the Examiner fails to consider all words in Appellants' claims as a whole during his patentability judgment. Appellants clearly claim "**a** software application" in Appellants' first element, and "**the** software application" in Appellants' fifth through eighth, and twelfth elements. Hence, Appellants are claiming the **same** software application in each of these elements. Appellants assert, however, that the Examiner does not view Appellants' "software application" on a consistent basis for each element and, therefore, the Examiner does not view claim 1 as a whole (discussed below).

Al-Salqan discloses a method and apparatus for encoding keys through interaction between a **user** and a security module. As such, Al-Salqan does not teach all of the limitations pertaining to Appellants' software application. The Examiner states that "Clear to those of ordinary skill in the art, the term "user" is a reference to a user employing a computer-implement application, an **interface to the security module** (see the Advisory Action mailed July 12, 2006, page 2, lines 18-19). Since the Examiner must consider all words in Appellants' claim 1, and since the Examiner must view Appellants' claim as a whole, the Examiner must consistently use the "interface to the security module" (hereinafter "security module interface") when viewing Appellants' software application limitation. As discussed below, the Examiner does not use the security module interface when viewing Appellants' software application and, therefore, the Examiner does not view Appellants' claim as a whole.

Regarding claim 1's sixth element, Appellants claim "determining, at the software application, that the encrypted tied key corresponds to the security module." This is due to the fact that if the software application has not received the encrypted tied key, the software application is required to request the encrypted tied key from the security module. The Examiner states that Appellants' limitation "does not indicate who or what does the determining and how such a determination is conducted" (see the Advisory Action mailed July 12, 2006, page 2, lines 34-35). Appellants disagree with the Examiner because, as claimed, the determination is done at the software application. Therefore, the software application has to perform the determination step.

The Examiner continues by stating that "Al-Salqan discloses the above limitations, as the correct password and a corresponding tied key of a user is passed to the security module via the software means for enabling such interaction between the user and security module" (see the Advisory Action mailed July 12, 2006, page 2, lines 36-38). Al-Salqan never teaches or suggests, however, that the security module interface performs any determination step whatsoever, let alone determining that the encrypted tied key corresponds to a security module as claimed by Appellants. If the software application receives results already determined (e.g., from a user), then the "determining" does not take place at the software application, which is different that what is claimed by Appellants. The Examiner does not suggest that Hosokawa teaches this limitation, and indeed Hosokawa does not teach such limitation.

Regarding claim 1's twelfth element, Appellants' claim "encrypting data provided by the software application using the recovered generated key." The Examiner states that Appellants' "provided by the software application" limitation is descriptive language describing data and has added no further structure to the claim (see the Advisory Action mailed July 12, 2006, page 2, lines 51-52). Appellants respectfully disagree with this assertion. This limitation has nothing to do with describing data itself, and everything to do with what is providing the data. MPEP 2106 (IV)(B)(1)(b) states:

> "Descriptive material that cannot exhibit any **functional interrelationship** with the way in which computing processes are performed does not constitute a statutory process, machine, manufacture or composition of matter and should be rejected under 35 U.S.C. 101. Thus, Office personnel should **consider the**

> **claimed invention as a whole** to determine whether the necessary functional interrelationship is provided."

Appellants' limitation of "provided by the software application" claims the functional interrelationship of the software application as it relates to the claim as a whole. Therefore, this limitation adds structure to the claim, and should be considered when viewing the claim. The Examiner states that "Al-Salqan discloses that such symmetric encryption keys are used to encrypt and decrypt data, and for such, **an application of software** is used" (see the Advisory Action mailed July 12, 2006, page 2, lines 18-19). This "application of software," however, is not the same as the security module interface that the Examiner used previously to reject Appellants' previous software application limitations. Therefore, the Examiner is not viewing Appellants' claim as a whole as asserted earlier. In addition, Al-Salqan never teaches or suggests that the **same** software application performs Appellants' first, fifth through eighth, and twelfth limitations as claimed by Appellants. The Examiner does not suggest that Hosokawa teaches these limitations, and indeed Hosokawa does not teach such limitations.

Based on the foregoing, Appellants respectfully submit that the rejection of each of Appellants' independent claims 1, 8, and 14 over Al-Salqan in view of Hosokawa has been overcome. Therefore, claims 1, 8, and 14 are allowable over Al-Salqan in view of Hosokawa. Claims 6-7, 19, 20, and 22 each depend, directly or indirectly, on one of the allowable independent claims 1, 8, and 14. Therefore, each of these claims is allowable over Al-Salqan in view of Hosokawa for at least the same reasons that the independent claims are allowable.

Claims 21, 23-24, 26-27, and 29 each depend, directly or indirectly, on one of the allowable independent claims 1, 8, and 14. The Examiner does not suggest that Appellants' admitted prior art teaches or suggests the limitations included in Appellants' allowable independent claims, and indeed Appellants' admitted prior does not teach such limitations. Therefore, each of claims 21, 23-24, 26-27, and 29 are allowable over Al-Salqan in view of Hosokawa and further in view of Appellants' admitted prior art for at least the same reasons that their respective independent claims are allowable.

Conclusion

For the foregoing reasons, Appellants respectfully submit that claims 1, 6-8, 14, and 19-29 are patentable, and, accordingly, Appellants respectfully request that the Examiner's claim rejections be reversed and claims 1, 6-8, 14, and 19-29 be allowed.

Respectfully submitted,

By /Leslie A. Van Leeuwen, Reg. No. 42,196/
Leslie A. Van Leeuwen, Reg. No. 42,196
Van Leeuwen & Van Leeuwen
Attorney for Appellants
Telephone: (512) 301-6738
Facsimile: (512) 301-6742

I. APPENDIX OF CLAIMS

1. A computer-implemented method for securing data, said method comprising:

receiving, at a security module, a first password corresponding to a software application;

generating, at the security module, a first mask value based on the first password;

combining, at the security module, the first mask value with a first encryption key, wherein the first encryption key is derived from a generated key and a known value, the combining resulting in a tied key;

encrypting, at the security module, the tied key using a second encryption key that is associated with the security module, the encrypting resulting in an encrypted tied key;

returning the encrypted tied key to the software application;

determining, at the software application, that the encrypted tied key corresponds to the security module;

in response to the determining, sending the encrypted tied key and a second password from the software application to the security module over a computer network, the second password being the same as the first password;

receiving, at the security module, the encrypted tied key and the second password from the software application;

in response to receiving the encrypted tied key and the second password, combining, at the security module, the encrypted tied key and the second password, the combining resulting in a recovered tied key;

generating a second mask value based on the second password;

separating a recovered encryption key from the recovered tied key using the second mask value, the recovered encryption key including a recovered generated key and a recovered known value; and

encrypting data provided by the software application using the recovered generated key.

6. The computer-implemented method as described in claim 1 further comprising:

determining whether the recovered known value is correct; and

processing a data file based on the determination.

7. The computer-implemented method as described in claim 6 wherein the processing is selected from the group consisting of encrypting the data file using the recovered generated key and decrypting the data file using the recovered generated key.

8. An information handling system comprising:

one or more processors;

a memory accessible by the processors;

one or more nonvolatile storage devices accessible by the processors;

a hardware security module accessible by the processors;

a data security tool for securing data using the hardware security module, the data security tool including:

means for receiving, at a security module, a first password corresponding to a software application;

means for generating, at the security module, a first mask value based on the first password using the hardware security module;

means for combining, at the security module, the first mask value with a first encryption key using the hardware security module, wherein the first encryption key is derived from a generated key and a known value, the combining resulting in a tied key;

means for encrypting, at the security module, the tied key using a second encryption key that is associated with the security module, the encrypting resulting in an encrypted tied key;

means for returning the encrypted tied key to the software application;

means for determining, at the software application, that the encrypted tied key corresponds to the security module;

in response to the determining, sending the encrypted tied key and a second password from the software application to the security module, the second password being the same as the first password;

means for receiving, at the security module, the encrypted tied key and the second password from the software application;

means for, in response to receiving the encrypted tied key and the second password, combining, at the security module, the encrypted tied key and the second password, the combining resulting in a recovered tied key;

means for generating a second mask value based on the second password using the hardware security module;

means for separating a recovered encryption key from the recovered tied key using the second mask value, the recovered encryption key including a recovered generated key and a recovered known value; and

means for encrypting data provided by the software application using the recovered generated key.

14. A computer program product stored in a computer operable media for securing data, said computer program product comprising:

means for receiving, at a security module, a first password corresponding to a software application;

means for generating, at the security module, a first mask value based on the first password using the hardware security module;

means for combining, at the security module, the first mask value with a first encryption key using the hardware security module, wherein the first encryption

key is derived from a generated key and a known value, the combining resulting in a tied key;

means for encrypting, at the security module, the tied key using a second encryption key that is associated with the security module, the encrypting resulting in an encrypted tied key;

means for returning the encrypted tied key to the software application;

means for determining, at the software application, that the encrypted tied key corresponds to the security module;

in response to the determining, sending the encrypted tied key and a second password from the software application to the security module, the second password being the same as the first password;

means for receiving, at the security module, the encrypted tied key and the second password from the software application;

means for, in response to receiving the encrypted tied key and the second password, combining, at the security module, the encrypted tied key and the second password, the combining resulting in a recovered tied key;

means for generating a second mask value based on the second password using the hardware security module;

means for separating a recovered encryption key from the recovered tied key using the second mask value, the recovered encryption key including a recovered generated key and a recovered known value; and

means for encrypting data provided by the software application using the recovered generated key.

19. The computer program product as described in claim 14 further comprising:

means for determining whether the recovered known value is correct; and

means for processing a data file corresponding to the determination.

20. The computer program product as described in claim 19 wherein the means for processing is selected from the group consisting of a means for encrypting the data file using the recovered generated key and a means for decrypting the data file using the recovered generated key.

21. The method of claim 1 wherein the security module is a separate hardware security module in a computer system.

22. The method of claim 1 wherein the generated key is at a level of security corresponding to a sensitivity level of the data being encrypted.

23. The method of claim 1 wherein encrypting the data is performed within the security module.

24. The information handling system of claim 8 wherein the security module is a separate hardware security module in a computer system.

25. The information handling system of claim 8 wherein the generated key is at a level of security corresponding to a sensitivity level of the data being encrypted.

26. The information handling system of claim 8 wherein encrypting the data is performed within the security module.

27. The computer program product of claim 14 wherein the security module is a separate hardware security module in a computer system.

28. The computer program product of claim 14 wherein the generated key is at a level of security corresponding to a sensitivity level of the data being encrypted.

29. The computer program product of claim 14 wherein encrypting the data is performed within the security module.

.

J. EVIDENCE APPENDIX

Not applicable.

K. RELATED PROCEEDINGS APPENDIX

Not applicable.